UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

BRITTANY WILEY, individually and on behalf of all others similarly situated, Plaintiff, v. ALTICE USA, INC., a New York Corporation, Defendant.	Case No. 1:20-CV-1297 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Brittany Wiley, individually and on behalf of all other similarly situated individuals, by and through her undersigned attorneys, Federman & Sherwood, files this Class Action Complaint against Altice USA, Inc. ("Altice" or "Defendant"), and allege the following based on personal knowledge, the investigation of counsel, and information and belief.

NATURE OF THE ACTION

1. Plaintiff and the other members of the Class (as defined below) are current and former employees ("Employees") and customers ("Customers") of Altice who entrusted Altice with their personally identifiable information ("PII"). Defendant betrayed Plaintiff's trust and that of the other Class Members by failing to properly safeguard and protect their PII and thereby enabling cyber criminals to steal their PII.

2. This class action seeks to redress Altice's unlawful and negligent disclosure of thousands of Employees' and Customers' PII in a major data breach in November 2019 (the "Data Breach" or "Breach"), in violation of common law and statutory obligations.

3. The Data Breach occurred as a result of a phishing campaign on Altice company email accounts. An undisclosed number of Altice employees, apparently ill-equipped to protect themselves, were tricked into providing their login information to the cyber criminals. With these credentials, the cyber criminals were able to remotely login to Altice company accounts, where they found a treasure trove of PII.

4. In one of the Altice accounts there was an unencrypted report that may have contained the PII of everyone who has ever worked for Altice or an Altice-owned company. At the very least, Altice has admitted that the report contained the PII of all current Employees—over 12,000 individuals—and many former Employees as well.

5. The PII on this report included Employees' names, employment information, dates of birth, Social Security numbers, and some drivers' license numbers. The PII of some customers was also stolen in the same Breach.

6. In short, thanks to Defendant's negligence and statutory violations, cyber criminals have everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

7. Plaintiff Wiley has already suffered identity theft as a result of the Data Breach, when someone used her Social Security number to file her taxes and steal her tax refund. This has cost her hundreds of dollars in the lost refund and incidental costs related to restoring her identity and a significant amount of lost time and opportunity.

8. For the rest of their lives, Plaintiff and the Class Members will have to deal with danger of identity thieves possessing their PII. Even those Class Members who have yet to experience identity theft are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred,

and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time, including missed opportunity for commissions, wasted paid-time off, lost time and expenses mitigating harms, increased risk of harm, diminished value of PII, loss of privacy, and/or additional damages as described below.

9. Accordingly, Plaintiff brings this action individually and on behalf of the Class, seeking actual damages, statutory damages, punitive damages, restitution, and injunctive and declaratory relief, along with the reasonable attorney fees, costs, and expenses incurred in bringing this action.

THE PARTIES

10. Plaintiff Brittany Wiley is domiciled in New York, and is a resident of Bronx County.

11. Defendant Altice USA, Inc. is incorporated in the State of Delaware and its principal place of business is Long Island City, New York.

JURISDICTION AND VENUE

12. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant.

13. This Court has personal jurisdiction over Defendant because its principal place of business is in this State, it regularly transacts business in this District, and Plaintiff and many Class Members reside in this District. Venue is likewise proper as to Defendant in this District because "a substantial part of the events or omissions giving rise to the claim occurred, or a substantial part of the property that is the subject of the action is situated." 28 U.S.C. § 1391(b)(2).

FACTUAL ALLEGATIONS

14. Plaintiff incorporates by reference all allegations of the paragraphs 1–6 as though fully alleged here.

A. Anatomy of a Data Breach

15. Although Altice has not yet disclosed the Breach to the public (or to investors), it has notified a few state attorneys general and has begun mailing letters to affected individuals. The following can be gleaned from these notices.[1]

16. Sometime in the fall of 2019, cyber criminals decided that Altice seemed like a juicy target for a phishing attack. So, these hackers initiated a phishing campaign.

17. Phishing attacks are common and most companies avoid falling victim to them by a combination of email protection software, regular employee trainings, and other common cyber security precautions.

18. In November 2019, the unsuspecting workers at Altice were wholly unprepared for this phishing attack. As can be seen from the notice, multiple Altice email accounts fell into the hands of cyber criminals.

19. The notice letter to the Vermont Attorney General (the "Notice") put it this way:

> **What happened?**
>
> In November 2019, an unauthorized third party gained access to certain Altice USA employees' email account credentials through a phishing incident. The unauthorized third party then used the stolen credentials to remotely access and, in some instances, download the employees' mailbox contents. . . .
>
> **What information was involved?**
>
> During our investigation, we learned in January 2020 that one of the downloaded mailboxes contained a password protected report that contained personal

[1] *See* Altice USA Inc Notice of Data Breach to Consumers, OFFICE OF VERMONT ATTORNEY GENERAL (Feb. 6, 2020), https://ago.vermont.gov/blog/2020/02/06/altice-usa-inc-notice-of-data-breach-to-consumers/.

> information, including name, employment information, Social Security number, date of birth and, in some instances, drivers' license number.[2]

20. The Notice then included alternative text block that stated either: "As a current employee, your personal information was included in this report." Or "As a former employee, your personal information was included in this report."[3]

21. Altice spokesperson has admitted that the unencrypted report contained the PII, including Social Security numbers, of all current employees. From the alternative "As a former employee" option in the letter, it is also apparent that this report foolishly contained the PII of *every former employee* as well. In other words, everyone who ever worked for Altice or its subsidiaries is a victim of this Data Breach.

22. Surprisingly, the Notice also states that Defendant has "no information at this time that would indicate that your personal information has been misused,"[4] as if cyber criminals downloading your personal information was not a misuse!

23. News reporting on the Data Breach provides additional details. In an article published on February 11, 2020, Newsday reported that the cyber criminals were able to steal the PII of "all 12,000 current employees."[5]

24. Newsday also reported that a small number of Altice customers had their PII exposed in the phishing attack. Altice is the provider of Optimum cable television and internet services.[6]

25. It is obvious that Altice negligently failed to take the necessary precautions required to safeguard and protect Plaintiff's and the other Class Members' PII from unauthorized

---

[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] James T. Madore, *Data breach exposes Altice employee, Optimum customer information*, NEWSDAY (Feb. 11, 2020 4:32 PM), https://www.newsday.com/business/altice-data-breach-employees-customers-1.41718432.
[6] *Id.*

disclosure. Defendant's actions represent a flagrant disregard of its Employees' and Customers' rights, both as to privacy and property.

26. Employees were obligated to provide Altice with their sensitive personal information, including their Social Security numbers.

27. Customers too were required to provide highly confidential PII to Altice.

B. Cyber Criminals Have Used and Will Continue to Use the Employees' and Customers' PII to Defraud Them

28. PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach can and will be used in a variety sordid ways for criminals to exploit Plaintiff and the Class Members and to profit off their misfortune.

29. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[7] For example, with the PII stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false identification and sell it to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and as many other harmful uses as there are identity thieves.[8] It hardly needs to be mentioned, but these criminal activities will result in devastating financial and personal losses to Plaintiff and the Class Members.

30. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals often trade the information on the cyber black-market for years.

[7]"Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[8]*See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

31. This was a financially motivated Breach, as the only reason the cyber criminals went through the trouble of running a targeted phishing campaign against Altice was to get the information that would enable them to engage in the kinds of criminal activity described in paragraph 22.

32. This is not just speculative. As the FTC has reported, if hackers get access to PII, they will use it.[9]

33. Hackers may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[10]

34. With this Data Breach, identity thieves have already started to prey on Altice Employees and Customers, and we can only anticipate that this will continue.

35. Identity theft victims like Plaintiff Wiley and other Class Members must spend countless hours and large amounts of money repairing the impact to their credit.[11]

36. Defendant's offer of one year of identity monitoring to Plaintiff and the Class is woefully inadequate. While some harm has begun already, as Plaintiff Wiley has already found out, the full scope of the harm has yet to be realized. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. Furthermore, identity monitoring only alerts someone to the fact that they have already been the

---

[9] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[10] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu (emphasis added).

[11] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's PII)—it does not prevent identity theft.[12]

37. As a direct and proximate result of the Data Breach, Plaintiff and the Class have suffered actual identity theft, and have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, and credit reports for unauthorized activity for years to come. Even more seriously is the identity restoration that Plaintiff Wiley and other Class Members must go through, spending countless hours filing police reports, filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiff and the Class must take.

38. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Actual identity theft, including fraudulent IRS tax returns;
b. Trespass, damage to, and theft of their personal property including PII;
c. Improper disclosure of their PII;
d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and having been already misused;

[12] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.

e. Damages flowing from Defendant untimely and inadequate notification of the data breach;

f. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their PII and that identity thieves have already used that information to defraud Plaintiff and members of the Class;

g. Ascertainable losses in the form of time taken off work to respond to identity theft and attempt to restore identity, including lost opportunity to earn commissions, wasted paid-time off, and lost wages from uncompensated time off;

h. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

i. Ascertainable losses in the form of deprivation of the value of customers' personal information for which there is a well-established and quantifiable national and international market;

j. The loss of use of and access to their credit, accounts, and/or funds;

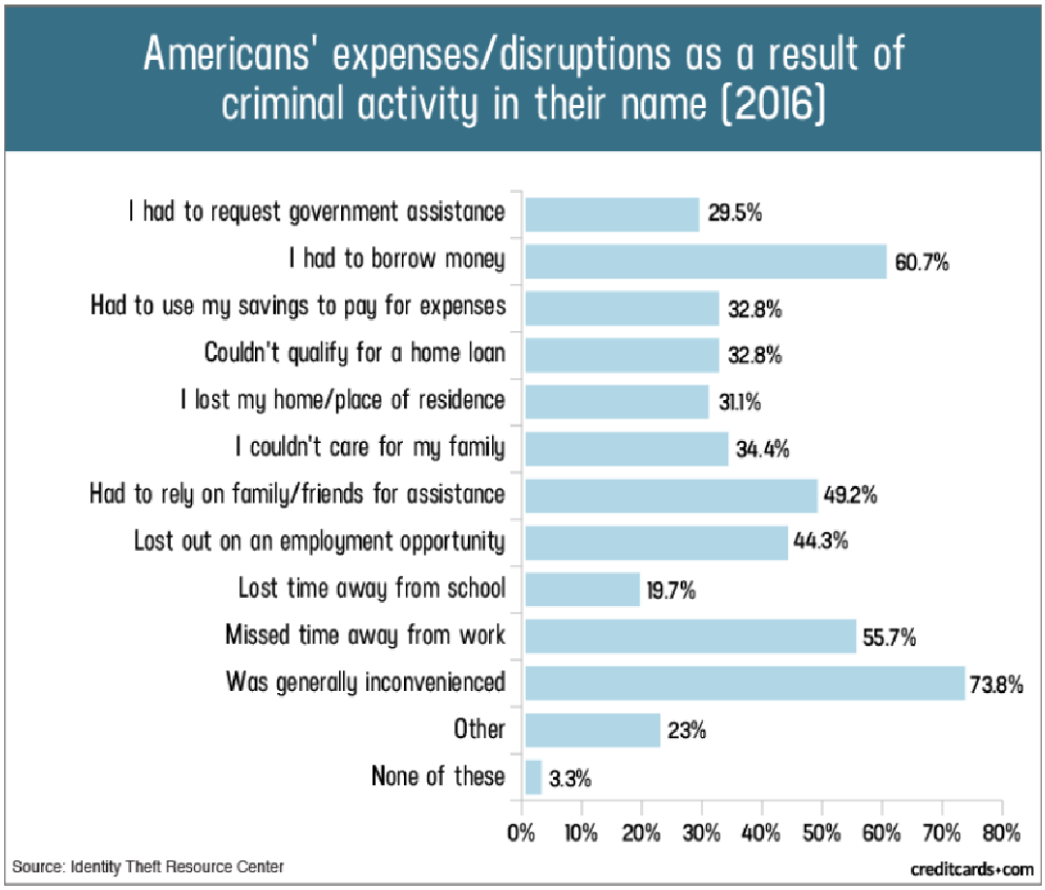
k. Damage to their credit due to fraudulent use of their PII; and

l. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

39. Below is a chart that shows the kinds of expenses and disruptions that victims of identity theft experience[13]:

[space intentionally left blank]

[13] Jason Steele, *Credit Card and ID Theft Statistics*, CREDITCARDS.COM (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.



40. Moreover, Plaintiff and Class have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards.

41. Defendant itself acknowledged the harm caused by the Data Breach because it offered Plaintiff and Class Members twelve months of identity theft repair and monitoring services. Twelve months of identity theft and repair and monitoring is, however, woefully inadequate to protect Plaintiff and Class Members from a lifetime of identity theft risk and does nothing to reimburse Plaintiff and Class Members for the injuries they have already suffered.

C. Defendant was Aware of the Risk of Cyber-Attacks and Could Have Prevented the Data Breach

42. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it.

43. The general public can tell you the names of some of the biggest data breaches: LabCorp, Quest Diagnostics, Yahoo, Equifax, Marriot International, Target, Home Depot, Anthem, Heartland Payment Systems, and TJX Companies, Inc.[14]

44. In requesting that Employees provide it with their most sensitive PII, Altice represented to its Employees that it understood the importance of protecting their PII and that it would do so in exchange for their employment. Upon information and belief, Altice emphasized to Employees and prospective employees through its stated privacy policies and company security practices that it maintained robust procedures designed to carefully protect the PII with which it was entrusted.

45. Further, New York law required that Altice—as a New York employer—protect its Employees' PII.

46. Likewise, as to its Customers, Altice on Optimum.net, assured them that their PII was in good hands, stating "Altice is committed to protecting the privacy of its customers."[15]

47. Altice represented to customers that it would protect their PII. It stated:

> We employ physical, electronic, and procedural safeguards to protect Subscriber Information. For example, we utilize secure socket layer (SSL) encryption to protect certain information you provide to us; employ verification measures to protect e-mail during delivery; maintain certain subscriber databases in restricted areas; and secure the content by use of firewalls and other security methods. We also limit access to databases containing subscribers' Personally Identifiable

[14] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.
[15] *Customer Privacy Notice*, OPTIMUM (effective Aug. 20, 2019), https://www.optimum.net/pages/PrivacyExisting.html.

> Information to specifically authorized employees and agents and other parties identified in the disclosure section above.[16]

Had Altice done as they promised, however, we would not be in this position.

48. In its Customer Privacy Notice Altice also acknowledges that it is a "cable operator" under the Cable Communications Act of 1984 ("Cable Act"), 47 U.S.C. § 551, *et seq.*, and that as a cable operator, it owes special statutory duties to its customers to protect their PII from unauthorized disclosure. *See* Cable Communications Act of 1984, 47 U.S.C. § 551(c). It states:

> The Cable Act imposes limitations with respect to the collection and disclosure of personally identifiable information by cable operators . . . . [C]able operators generally may not disclose personally identifiable information without consent of the subscriber concerned. Also, cable operators must take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator. If we violate your rights, you may be entitled to bring a civil action in a federal court, which may award actual, liquidated, and punitive damages, fees and costs, and other remedies that may be available.[17]

49. Data breaches are preventable.[18] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[19] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[20]

50. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information

---

[16] *Id.*
[17] *Id.*
[18] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)
[19] *Id.* at 17.
[20] *Id.* at 28.

security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[21]

51. In a Data Breach like this, many failures laid the groundwork for the success (from the cyber criminal's view) of the Breach. For example, Altice's email protection software was not sufficient to recognize and block the phishing emails, even though multiple employees were receiving the same kind of emails at once (a red flag often marked by good email protection systems). Also, multiple employees either forgot their anti-phishing training or, more likely, were inadequately trained in identifying, reporting, and deleting phishing emails.

52. Altice additionally had far too much information held in unencrypted email accounts. No sophisticated business in the 21st century should permit a document containing the PII of all 12,000+ of its current employees to be stored—unencrypted—in company email inboxes.

53. And reasonable care dictates that a business would dispose of all former employee's information as soon as it is no longer needed, and until then it should be segregated into an encrypted system, separate from the email servers. None of this information should have been stored in unencrypted documents that were emailed around the company network.

54. Altice, rather than following this basic standard of care, apparently kept the PII of former employees forever in an unencrypted report that it permitted to be mailed around company email network. Employees who left the company

55. Email phishing attacks are one of the most common and preventable kinds of cyberattacks. As a large, publicly-traded company, with obligations to its shareholders in addition to its 12,000 employees and 5 million customers, one would have thought that Altice would have

[21] *Id.*

at least complied with the industry security standards for *small* businesses. But, as described below, it did not.

56. One of the best protections against email related threats is security awareness training and testing on a regular basis. This should be a key part of a company's on-going training of its employees. "[S]ince phishing is still a significant, initial point of compromise, additional work needs to be done to further lower the click rate. . . . This can be done through more frequent security awareness training, phishing simulation, and better monitoring of metrics pertaining to phishing (including whether there are any particular repeat offenders)."[22]

57. ProtonMail Technologies publishes a guide for IT Security to small businesses (i.e., companies with far less PII to protect than Altice). In its 2019 guide, ProtonMail dedicates a full chapter of its ebook guide to the danger of phishing and ways a small business can avoid prevent falling prey to a phishing attack. It reports:

> Phishing and fraud are becoming ever more extensive problems. A recent threat survey from the cybersecurity firm Proofpoint stated that between 2017 and 2018, email-based attacks on businesses increased 476 percent. The FBI reported that these types of attacks cost companies around the world $12 billion annually.
>
> Similar to your overall IT security, your email security relies on training your employees to implement security best practices and to recognize possible phishing attempts. This must be deeply ingrained into every staff member so that every time they check their emails, they are alert to the possibility of malicious action.[23]

58. The guidance that ProtonMail provides small businesses is likely still not adequate for a company like of Altice, with added obligations under the heightened standard of the New York Labor Law and the Cable Communications Act of 1984, and the increased danger from the sensitivity and wealth of PII that Altice retains, but ProtonMail's guidance is informative for

[22]Aaron Jensen, *Healthcare Phishing Statistics: 2019 HIMSS Survey Results*, PROOFPOINT (Mar. 27, 2019), https://www.proofpoint.com/us/security-awareness/post/healthcare-phishing-statistics-2019-himss-survey-results.
[23]*The ProtonMail Guide to IT Security for Small Businesses*, PROTONMAIL (2019), available at https://protonmail.com/it-security-complete-guide-for-businesses.

showing how inadequately Altice protected the PII of the Plaintiffs and the Class. ProofPoint lists numerous tools under the heading, "How to Prevent Phishing":

a. **Training:** "Training your employees on how to recognize phishing emails and what to do when they encounter one is the first and most important step in maintaining email security. *This training should be continuous* . . . ."

b. **Limit Public Information:** "Attackers cannot target your employees if they don't know their email addresses. Don't publish non-essential contact details on your website or any public directories . . . .

c. **Carefully check emails:** "First off, your employees should be skeptical anytime they receive an email from an unknown sender. Second, most phishing emails are riddled with typos, odd syntax, or stilted language. Finally, check the 'From' address to see if it is odd . . . . If an email looks suspicious, employees should report it."

d. **Beware of links and attachments:** "Do not click on links or download attachments without verifying the source first and establishing the legitimacy of the link or attachment. . . ."

e. **Do not automatically download remote content:** "Remote content in emails, like photos, can run scripts on your computer that you are not expecting, and advanced hackers can hide malicious code in them. You should configure your email service provider to not automatically download remote content. This will allow you to verify an email is legitimate before you run any unknown scripts contained in it."

f. **Hover over hyperlinks:** "Never click on hyperlinked text without hovering your cursor over the link first to check the destination URL, which should appear in the lower corner of your window. Sometimes the hacker might disguise a malicious link as a short URL." [Proofpoint notes that there are tools online available for retrieving original URLs from shortened ones.]

g. If in doubt, investigate: "Often phishing emails will try to create a false sense of urgency by saying something requires your immediate action. However, if your employees are not sure if an email is genuine, they should not be afraid to take extra time to verify the email. This might include asking a colleague, your IT security lead, looking up the website of the service the email is purportedly from, or, if they have a phone number, calling the institution, colleague, or client that sent the email."

h. Take preventative measures: "Using an end-to-end encrypted email service gives your business's emails an added layer of protection in the case of a data breach. A spam filter will remove the numerous random emails that you might receive, making it more difficult for a phishing attack to get through. Finally, other tools, like Domain-based Message Authentication, Reporting, and Conformance (DMARC) help you be sure that the email came from the person it claims to come from, making it easier to identify potential phishing attacks."[24]

59. As mentioned, these are basic, common-sense email security measures that ever business, especially large, publicly traded businesses, should be doing. Altice, with its duties under New York labor law and the Cable Communication Act should be doing even more. But by adequately taking these common sense solutions, Altice could have prevented this Data Breach from occurring.

D. Altice's Response to the Data Breach is Inadequate to Protect Plaintiff and the Class

60. Altice failed to inform Plaintiff and Class Members of the Data Breach in time for them to protect themselves from identity theft.

[24] *Id.*

61. Altice stated that it discovered the Data Breach in November 2019. It did not disclose how long the cyber criminals had access to the company accounts or the precise day when Altice discovered the Breach. The notice letters sent to Plaintiff and Class Members stated that Altice did not learned of the existence of the report until January 2020, two months after it discovered the Data Breach. And yet, Altice did not start notifying Employees and affected Customers until February 2020.

62. During these intervals, the cyber criminals were more diligent at exploiting the information than Altice was at investigating the Data Breach. Because in January 2020, identity thieves had already begun filing false tax returns with the stolen names and Social Security Numbers.

63. If Altice had investigated the Data Breach more diligently and reported it sooner, the damage could have been mitigated.

64. Also, the letter Altice sent employees was in an inconspicuous envelope with nothing on the outside sufficient to notify its recipients of the vital importance of what was inside. This naturally resulted in some affected individuals disregarding the envelope with the piles of junk mail that have long filled the recycling bins of 21st Century Americans.

65. As discussed above, the 12-months of identity theft monitoring is seriously inadequate for the risks to which Altice has exposed its Employees and Customers. It has also not offered to compensate Employees for lost time or provide additional paid time off for Employees responding to identity theft, or other assistance for Employees dealing with the IRS, state tax agencies, or federal, state, and local law enforcement. And Altice has certainly not offered to reimburse Plaintiff Wiley or other Class Members for any costs incurred as a result of falsely filed tax returns.

E. Plaintiff's Experience

66. The risks and harms described above have already begun happening to Plaintiff and other members of the Class.

67. Plaintiff's experiences are not exactly the kind of experiences that every other Class Member has or will experience from this Data Breach.

68. Plaintiff Wiley is a current employee of Altice. On February 10, 2020, she received an inconspicuous envelope in the mail from Altice. Although not sure if it was legitimate, she opened it and was shocked to find out that she was the victim of a data breach.

69. On February 12, 2020, Plaintiff Wiley tried to file her tax return through TurboTax filing software, but her tax return was rejected. TurboTax reported that "A tax return has already been filed with the IRS using the same SSN."

70. Plaintiff Wiley discovered that an identity thief with access to her Social Security number had filed her tax return in January 2020.

71. Plaintiff Wiley was relying upon the tax refund to pay for a large bill that will soon come due. Now, when the bill comes due, she will be unable to pay it and may incur late fees and additional penalties.

72. Since this discovery, Plaintiff Wiley has spent hours on the phone with the Internal Revenue Service, filing a police report at her local precinct, and seeking and reading advice on identity restoration.

73. This time responding to the Data Breach and related identity theft has caused her to miss commissions and thus earn less money than she would have been able to.

74. She is desperately trying to mitigate the damage that Altice has caused her but is certain to incur additional damages in the form of lost time and expenses for identity restoration.

And, because identity thieves have her PII, she will need to have identity theft monitoring protection for the rest of her life, and may need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[25]

CLASS ACTION ALLEGATIONS

75. Plaintiff incorporates by reference all preceding paragraphs as if fully restated here.

76. Plaintiff brings this action against Altice on behalf of herself and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of a nationwide Class defined as follows:

> **All persons whose personally identifiable information was compromised as a result of the Data Breach at Altice USA, Inc. in November 2019.**

77. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

78. Plaintiff reserves the right to amend the above definition or to propose other or additional subclasses, including a Customer subclass, in subsequent pleadings and motions for class certification.

a. Class Certification is Appropriate

79. The proposed Class and any additional subclasses meet the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

[25] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

80. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. Defendant has not admitted the total number of individuals affected, but based on what Defendant has disclosed, the Class contains more than 12,000 persons.

81. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Altice's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive PII compromised in the same way by the same conduct of Altice.

82. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the class that she seeks to represent; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel.

83. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the class individually to effectively redress Altice's wrongdoing. Even if class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and

provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

84. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's PII;

c. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their PII, and whether it breached this duty;

d. Whether Altice violated state and federal laws, thereby breaching its duties to Plaintiff and the Class as a result of the Data Breach;

e. Whether Altice failed to provide adequate email security filtering;

f. Whether Altice failed to provide adequate anti-phishing training to its employees;

g. Whether Altice knew or should have known that its computer and network security systems were vulnerable to phishing attacks;

h. Whether Altice's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company email accounts;

i. Whether Altice was negligent in permitting an unencrypted report containing the PII off vast numbers of individuals to be stored within its unencrypted email accounts;

j. Whether Altice was negligent in failing to adhere to reasonable retention policies, there by greatly increasing the size of the Data Breach to include former Employees;

k. Whether Altice breached contractual duties to Employees and Customers to use reasonable care in protecting their PII;

l. Whether Altice failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

m. Whether Altice continues to breach duties to Plaintiff and the Class;

n. Whether Plaintiff and the Class suffered injury as a proximate result of Altice's negligent actions or failures to act; and

o. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of the Class)

85. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

86. Defendant Altice solicited, gathered, and stored the PII of Plaintiff and the Class.

87. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed. Defendant had a duty to Plaintiff and each Class member to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiff and the Class Members were the

foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class Members had no ability to protect their PII that was in Altice's possession.

88. Defendant was well aware of the fact that cyber criminals routinely target large corporations through phishing attacks and other cyberattacks in an attempt to steal employee and customer PII.

89. Defendant owed Plaintiff and the Class member a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

90. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts, including those in New York and the Second Circuit, and legislatures, including New York's, have recognized the existence of a specific duty to reasonably safeguard personal information.

91. Defendant had duties to protect and safeguard their PII from being vulnerable to phishing attacks, including by using adequate email filtering software, providing adequate and frequent training to employees on identifying, avoiding, and reporting suspicious emails; by using encrypted email accounts, by encrypting any document or report containing PII, by not permitting documents containing PII to be attached to or stored in emails, and other similarly common-sense

precautions when dealing with sensitive PII. Additional duties that Altice owed Plaintiff and the Class include:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession;

b. To protect the PII in its possession using reasonable and adequate security procedures and systems;

c. To adequately and properly audit, test, and train its employees to avoid phishing emails;

d. To use adequate email security systems, including industry standard SPAM filters, DMARC enforcement, and/or Sender Policy Framework enforcement, to protect against phishing emails;

e. To adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;

f. To train its employees not to store PII in their email inboxes longer than absolutely necessary for the specific purpose that it was sent or received;

g. To implement processes to quickly detect a data breach, security incident, or intrusion; and

h. To promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

92. Plaintiff and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and Altice. Defendant was in a position to ensure that its systems were sufficient to protect the PII that Plaintiff and the Class had entrusted to it.

93. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class Members' PII. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the PII in its possession;

b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees to avoid phishing emails;

d. Failing to use adequate email security systems, including industry standard SPAM filters, DMARC enforcement, and/or Sender Policy Framework enforcement, to protect against phishing emails;

e. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store PII;

f. Failing to adequately and properly train its employees not to store PII in their email inboxes, and certainly not longer than absolutely necessary for the specific purpose that it was sent or received;

g. Failing to consistently enforce security policies aimed at protecting Plaintiff and the Class's PII;

h. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

i. Failing to abide by reasonable retention and destruction policies for PII of former employees; and

j. Failing to promptly notify Plaintiff and Class Members of the Data Breach that affected their PII.

94. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

95. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

96. The damages Plaintiff and the Class have suffered (as alleged above) were and are reasonably foreseeable.

97. The damages Plaintiff and the Class have and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

98. Plaintiff and the Class have suffered injury and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE* – *N.Y. LABOR LAW*
(On Behalf of the Class, or alternatively, an Employee Subclass)

99. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

100. As a New York company, Defendant had a duty under New York Labor Law § 203-D to protect its Employees' PII, including Social Security numbers, from public posting or displaying, storing it in files with unrestricted access, or communicating it to the general public.

101. Defendant violated these duties in its actions and inactions that resulted in the Data Breach.

102. The harm that has occurred is the type of harm the NY Labor Law was intended to guard against.

103. Plaintiff and the Class Members who are or were employees of Defendant are within the class of persons who the NY Labor Law was intended to protect.

104. Defendant's breach of these duties was knowing, because it had not put in place "any policies or procedures to safeguard against such violation, including procedures to notify relevant employees of these provisions." N.Y. Labor Law § 203-D(3).

105. Plaintiff and the Class have suffered damages as a result of Defendant's breaches of its duties, and the damages were foreseeable.

106. Defendant's violations of these duties are the proximate cause of Plaintiff's and the Class Members' damages.

107. Plaintiff and the Class are entitled to actual and punitive damages for Defendant's negligence *per se* in an amount to be proven at trial.

THIRD CAUSE OF ACTION
NEGLIGENCE *PER SE* – *CABLE ACT*
(On Behalf of the Class, or alternatively, a Customer Subclass)

108. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

109. As a cable subscriber, Defendant had a duty under the Cable Communications Act of 1984, 47 U.S.C. § 551 to "not disclose" its customers' PII, including Social Security numbers, without prior written permission and to "take such actions as are necessary to prevent unauthorized access to such information." 47 U.S.C. § 551(c)(1).

110. Plaintiff, and many other members of the Class (including current and former Employees) are or were subscribers of Defendant's cable television products.

111. Defendant violated its duties under the Cable Act by Defendant's actions and inactions that resulted in the Data Breach.

112. The harm that has occurred is the type of harm the Cable Act was intended to guard against.

113. Plaintiff and the Class Members who are or were subscribers of Defendant's cable television products are within the class of persons who the Cable Act was intended to protect.

114. Plaintiff and the Class have suffered damages as a result of Defendant's breaches of its duties, and the damages were foreseeable.

115. Defendant's violations of these duties are the proximate cause of Plaintiff's and the Class Members' damages.

116. Plaintiff and the Class are entitled to actual and punitive damages for Defendant's negligence *per se* in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
NEGLIGENCE *PER SE* – *BREACH NOTICE*
(On Behalf of the Class, or alternatively, a Customer Subclass)

117. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

118. Under New York law, Defendant had a duty to notify Plaintiff and the Class of the Data Breach in the "most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measure necessary to determine the scope of the breach and restore the reasonable integrity of the system." N.Y. Gen. Bus. Law § 899-aa(2), (4).

119. Defendant violated this duty when it failed to timely notify Plaintiff and the Class Members of the Data Breach, instead taking around three months to warn them of their imminent risk of identity theft.

120. Defendant discovered the Data Breach in November 2019. It took until January 2020, around two months, for Defendant to get around to identifying that a report containing all

current and possibly all former Employees was contained within an affected email inbox. Defendant then waited another month before notifying affected individuals.

121. During the interval, cyber criminals were able to commit identity theft on Plaintiff and other Class Members who would have been able to protect themselves had they been warned earlier.

122. The harm that Defendant's untimely notice caused is the type of harm the N.Y. Breach Notice law was intended to guard against.

123. Plaintiff and the Class Members are within the class of persons who the Cable Act was intended to protect.

124. Plaintiff and the Class have suffered damages as a result of Defendant's breaches of its duties, and the damages were foreseeable.

125. Defendant's violations of these duties are the proximate cause of Plaintiff's and the Class Members' damages.

126. Plaintiff and the Class are entitled to actual and punitive damages for Defendant's negligence *per se* in an amount to be proven at trial.

FIFTH CAUSE OF ACTION
BREACH OF CONTRACT OR IMPLIED CONTRACT
(On Behalf of an Employee Subclass)

127. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

128. Plaintiff alleges this count in the alternative to the Negligence and Negligence Per Se counts and in addition to the New York Labor Law and Cable Act counts.

129. Plaintiff and Class Members who are or were employees of Altice were required, as a condition of their employment to provide Defendant with their PII, including their Social Security numbers.

130. Class Members who are or were customers of Altice were required as part of their contract to provide Altice with their PII.

131. Based on Defendant's representations and acceptance of Plaintiff's and the Class Members' PII, Defendant had express and/or implied duty that was a material part of their contracts to safeguard their PII through the use of reasonable industry standards.

132. Defendant's failure to protect the PII of Plaintiff and Class Members who are employees constitutes a material breach of the terms of the agreement by Defendant.

133. As a direct and proximate result of Defendant's breach of express or implied contract, Plaintiff and the Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiff's and the Class Members' PII.

SIXTH CAUSE OF ACTION
NEW YORK LABOR LAW § 203-C
(On Behalf of an Employee Subclass)

134. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

135. Plaintiff brings this count on behalf of herself and Class Members who are or were employees of Altice.

136. Under New York law, "[a]n employer shall not unless otherwise required by law: . . . (a) Publicly post or display an employee's social security number; . . . (c) Place a social security number in files with unrestricted access; or (d) Communicate an employee's personal identifying information to the general public." N.Y. Labor Law § 203-d(1).

137. "[P]ersonal identifying information" is defined as including an individual's "social security number, home address or telephone number, personal electronic mail address, Internet

identification name or password, parent's surname prior to marriage, or drivers' license number." *Id.* § 203-d(1)(d).

138. The statute further provides that "[i]t shall be presumptive evidence that a violation of this section was knowing if the employer has not put in place any policies or procedures to safeguard against such violation, including procedures to notify relevant employees of these provisions." *Id.* § 203-d(3).

139. Defendant's acts and omissions were unlawful and in violation of N.Y. Labor Law § 203-d because Defendant sent a file containing thousands of Employees and Customers' PII, including Social Security numbers, on its unencrypted email accounts, and stored it on the same unencrypted email inboxes.

140. The report containing the Employee and Customer PII was unencrypted and not adequately password protected, as evidenced by the hackers' prompt circumvention of the password that was on the report.

141. Defendant, moreover, did not put into place any policies or procedures—despite its covenants stating otherwise—to safeguard against such violations, as is made evident by Defendant's susceptibility to a phishing scam (of which it should have been aware by way of even minimal data security training), the fact that the files containing all of its current and former employee's PII were emailed in unencrypted format, and—rather than destroy its former Employees' PII as is a basic data security practice—Altice continued to store in its files former Employee's PII.

142. Accordingly, Plaintiff on behalf of herself and the Class Members who are or were employees of Altice, are entitled to statutory damages, compensatory damages, injunctive relief, and reasonable attorney fees and costs for Altice's violations of N.Y. Labor Law § 203-c(3).

SEVENTH CAUSE OF ACTION
CABLE COMMUNICATIONS ACT OF 1984
(On Behalf of the Class, or alternatively a Subscriber Subclass)

143. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

144. Plaintiff brings this count on behalf of herself and Class Members who are also Subscribers to Defendant's cable television products.

145. As Defendant acknowledges, it is a "cable provider" as defined in the Cable Communications Act of 1984 (Cable Act), 47 U.S.C. § 551.

146. As part of its employment agreements with Defendant, Plaintiff and Class Members who are employees were offered by Defendant cable television subscriber benefits, including discounted rates. As such, Plaintiff and Class Members are or were "cable subscribers" under the Cable Act, as well as Employees.

147. Plaintiff is a cable subscriber with Defendant.

148. The Cable Act provides that "a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned ***and shall*** take ***such actions as are necessary to prevent unauthorized access*** to such information by a person other than the subscriber or cable operator." 47 U.S.C. § 551(c)(1) (emphasis added).

149. Defendant violated this provision by failing to take the necessary precautions to prevent the Data Breach.

150. As a result of Defendant's violation of § 551(c)(1), Plaintiff and the Class Members who are or were cable subscribers have suffered damages.

151. The Cable Act also provides that "[a] cable operator shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected . . . ." *Id.* § 551(e).

152. Defendant violated this provision by failing to destroy the PII of Class Members who were former Employees and were also, during their employment, subscribers with Defendant's cable television service.

153. The Cable Act provides that "[a]ny person aggrieved by any act of a cable operator in violation of this section *may bring a civil action in a United States district court*." *Id.* § 551(f)(1).

154. Plaintiff and the Class were aggrieved by Defendant's violations of the Cable Act and have suffered damages. They are therefore entitled to "actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher; punitive damages; and reasonable attorneys' fees and other litigation costs reasonably incurred." *Id.* § 551(f)(2).

155. These remedies are cumulative to all other lawful remedies. *Id.* § 551(f)(3).

EIGHTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of the Class)

156. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

157. Defendant, by way of its affirmative actions and omissions, including its knowing violations of its express or implied contracts with Plaintiff and the Class Members, New York Labor Law and the Cable Act, knowingly and deliberately enriched itself by saving the costs it reasonably and contractually should have expended on data security measures to secure Plaintiff's and Class Members' PII.

158. Instead of providing for a reasonable level of security that would have prevented the Data Breach, as described above and is common industry practice among companies entrusted with similar PII, Defendant instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiff and Class Members.

159. Upon information and belief, Defendant deliberately cut every penny and canceled every support contract that it could to make its earnings look good for its shareholders when these actions were setting the company up to be exceptionally vulnerable to a data breach.

160. While it cut costs on security, Defendant continued to obtain the benefits conferred on it by Plaintiff's and Class Members employment and subscriptions.

161. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result. As a result of Defendant's decision to profit rather than provide requisite security and the resulting disclosure of Employees' and Customers' PII, Plaintiff and Class Members suffered and continue to suffer considerable injuries as alleged in detail above.

162. Defendant therefore engaged in an opportunistic material breach of contract, wherein it profited from interference with Plaintiff's and Class Members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its breach.

163. Accordingly, Plaintiff on behalf of herself and the Class Members, is entitled to relief in the form of restitution and/or compensatory damages.

NINTH CAUSE OF ACTION
INJUNCTIVE AND DECLARATORY RELIEF
(On Behalf of the Class)

164. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

165. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

166. As previously alleged and pleaded, Defendant owes duties of care to Plaintiff and Class Members that requires it to adequately secure their PII.

167. Defendant still possesses the PII of Plaintiff and the Class Members.

168. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class.

169. Defendant has claimed that it is taking some steps to increase its data security, but there is nothing to prevent Defendant from reversing these changes once it has weathered the increased public attention resulting from this Breach, and to once again place profits above protection.

170. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering Defendant to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
b. Ordering Defendant to engage third-party security auditors and internal personnel to run automated security monitoring;
c. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

d. Ordering that Defendant's segment employee and customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant cease transmitting PII via unencrypted email;

f. Ordering that Defendant cease storing PII in email accounts;

g. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner Customer and Employee data not necessary for its provisions of services;

h. Ordering that Defendant conduct regular database scanning and securing checks;

i. Ordering Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

j. Ordering Defendant to implement and enforce adequate retention policies for PII, including destroying Customer and Employee PII as soon as it is no longer necessary for the it to be retained; and

k. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class

counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual and statutory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Complaint.

Dated: February 13, 2020

Respectfully submitted,

/s/ *William B. Federman*

William B. Federman
(S.D. New York #WF9124)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
(405) 235-1560
(405) 239-2112 (facsimile)
wbf@federmanlaw.com

Counsel for Plaintiff Brittany Wiley and the Putative Class